10/805,168
10/05/04

Europäisches Patentamt | European Patent Office | Office européen des brevets

Bescheinigung | Certificate | Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. | Patent application No. | Demande de brevet n°

03425172.8

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

Anmeldung Nr:
Application no.: 03425172.8
Demande no:

Anmeldetag:
Date of filing: 19.03.03
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

STMicroelectronics S.r.l.
Via C. Olivetti, 2
20041 Agrate Brianza (Milano)
ITALIE

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

Method for performing error corrections of digital information codified as a symbol sequence

In Anspruch genommene Priorität(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/ Classification internationale des brevets:

H03H13/00

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT RO SE SI SK TR LI

Titolo: Metodo per effettuare correzioni d'errore su informazioni digitali codificate come sequenze di simboli.

DESCRIZIONE

Campo di applicazione

Nel suo aspetto più generale la presente invenzione riguarda un metodo per applicare la teoria dei codici autocorrettori ad informazioni digitali codificate come sequenze di simboli, ad esempio in logica booleana, memorizzate in sistemi di memoria elettronici o trasmesse da e verso tali sistemi.

Più in particolare, l'invenzione riguarda un metodo del tipo suddetto e in cui è prevista la trasmissione di sequenze incorporanti una porzione di codice correttore d'errore che consenta di ricostruire in ricezione la sequenza che più probabilmente è l'originale trasmessa mediante il calcolo di una sindrome d'errore utilizzando una matrice di parità.

Arte nota

Nello specifico settore tecnico dei sistemi di comunicazioni è noto che un qualunque messaggio comprendente informazioni digitali può essere elaborato e trasferito da un sistema ad un altro mediante mezzi elettronici di comunicazione che possono essere affetti da rumore.

In sostanza, una sequenza $\underline{x}$ di simboli booleani trasmessi attraverso un canale di comunicazione soggetto a rumore può pervenire in ricezione come una diversa sequenza $\underline{y}$ dalla quale occorre risalire alla sequenza iniziale $\underline{x}$.

Normalmente, la sequenza $\underline{x}$ di simboli da trasmettere comprende una porzione aggiuntiva o ridondante includente un codice correttore d'errore che consente di ricostruire in ricezione il messaggio che più probabilmente è l'originale anche in presenza di errori.

Questi codici correttori d'errore sono basati su ben note teorie matematiche, come ad esempio la teoria dei codici di Hamming, che sono attualmente applicate in molti contesti in cui si ha l'esigenza di rimediare alla presenza di rumore nei canali di comunicazione.

Per meglio comprendere tutti gli aspetti della presente invenzione, qui di seguito viene presentata una dettagliata descrizione delle metodologie maggiormente in uso per la correzione di errori in informazioni digitali codificate come sequenze di simboli in logica booleana.

0.1 Definizioni basilari

Definizione 1 *Dati $m \cdot n$ numeri reali, si chiama* matrice *del tipo* $[m \times n]$ *una tabella come la seguente:*

$$M = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

Definizione 2 *Si chiama* trasposta *della matrice sopra e si indica M^T, la matrice:*

$$\begin{pmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{m2} \\ \vdots & & & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{mn} \end{pmatrix}$$

che si ottiene da M scambiando, ordinatamente, le righe con le colonne

Definizione 3 *Consideriamo una matrice quadrata M di ordine $n \times n$. Fissato un elemento a_{ik} della matrice M, e soppressa in essa la riga e la colonna che in esso si incrociano (la i-esima riga e la j-esima colonna) si ottiene una matrice quadrata di ordine $(n-1) \times (n-1)$, il cui determinante si chiama* minore complementare *di a_{ik} e verrà indicato con M_{ik}.*

Definizione 4 *Si chiama* determinante *della matrice del secondo ordine il numero:*

$$a_{11}a_{22} - a_{12}a_{21}$$

Definizione 5 *Si chiama determinante di una matrice di ordine n:*

$$\sum_{k=1}^{n} a_{ik} \cdot (-1)^{i-k} M_{ik}$$

Definizione 6 *La matrice quadrata che ha 1 come elementi a_{ii} e 0 altrove è detta* matrice identità *e viene indicata con I.*

Definizione 7 *Un* gruppo $\mathbf{G}$ *è un insieme, dove è definita un'operazione* $*$ *per cui:*

i- $\mathbf{G}$ *è chiuso per* $*$*, cioè se* $g \in \mathbf{G}$ *e* $h \in \mathbf{G} \Longrightarrow g * h \in \mathbf{G}$*;*

ii- $*$ *è associativa;*

iii- $\mathbf{G}$ *ha l'identità, cioè* $\exists e \in \mathbf{G}$ *tale che* $e * g = g * e = g \ \forall g \in \mathbf{G}$*;*

iv- $\forall g \in \mathbf{G}$ *esiste l'inverso, cioè* $\exists g^{-1} \in \mathbf{G}$ *tale che* $g^{-1} * g = g * g^{-1} = e$*.*

Definizione 8 *Se l'operazione* $*$ *è la somma il gruppo è detto additivo.*

Definizione 9 *Un gruppo si dice* abeliano *se l'operazione* $*$ *è commutativa.*

Definizione 10 *Si dice* classi di resto $(\mathrm{mod}\ p)$ *e si indica* $\mathbb{Z}_p$ *l'insieme* $\{0, 1, 2, \cdots, p-1\}$*, la proprietà è che in queste classi* p *= identità.*

Definizione 11 *Un* gruppo booleano *è un gruppo binario, cioè un gruppo dove sono presenti solo i numeri 0 e 1 e 1+1=0.*

Definizione 12 *Un insieme di vettori* $v_1, \cdots, v_k$ *è* linearmente dipendenti *se e solo se ci sono degli scalari* $c_1, \cdots, c_k \neq 0$ *tale che* $c_1v_1 + c_2v_2 + \cdots + c_kv_k = 0$*.*

Definizione 13 *Una famiglia di vettori si dice* base *dello spazio se è una famiglia generatrice, cioè ogni altro vettore dello spazio si trova come combinazione lineare di questi vettori, ed è costituita da vettori linearmente indipendenti.*

0.1.1 I codici

Il soggetto della teoria dei codici autocorrettori, una branca della teoria dell'informazione, è nato originariamente per rispondere ad alcuni problemi pratici nella comunicazione di informazioni digitali codificate. Si consideri un messaggio come un blocco di simboli di un alfabeto finito; di solito è una sequenza di 0 e 1 ma può essere anche un numero qualsiasi, una lettera o una

frase completa. Il messaggio è trasmesso attraverso un canale di comunicazione che è soggetto a rumore. L'oggetto della teoria dei codici autocorrettori è aggiungere dei termini ridondanti al messaggio cosicchè si possa risalire al messaggio originale se quello trasmesso è stato danneggiato. Innanzitutto si deve fare una distinzione tra diagnosticare e correggere gli errori. La diagnostica riconosce la presenza di un errore, mentre la correzione riconosce e corregge l'errore.
Ogni messaggio chiamato c consiste di k digit di informazione. La codifica trasforma, secondo certe regole, ogni messaggio di input c in una n-pla binaria x con $n > k$.
Questa n-pla binaria x è la parola codice del messaggio c. Durante la trasmissione possono avvenire degli errori, si riceve dunque una n-pla binaria y

$$c \rightarrow x \rightarrow \boxed{\text{canale}} \rightarrow y$$

Consideriamo ora lo spazio $\mathbf{V}$ di tutte le n-ple di 0 e 1 con l'addizione di vettori componente per componente modulo 2.

Definizione 14 *Un* $[n, k]$ *codice* lineare *binario è l'insieme di tutte le combinazioni lineari di* $k(\neq 0)$ *vettori indipendenti in* $\mathbf{V}$. *Lineare indica che se due o più vettori sono nel codice, lo è anche la loro somma.*

Definizione 15 *Una* matrice generatrice G *per un codice lineare è una matrice* $k \times n$ *le cui righe sono una base per* C.

Definizione 16 *Una* matrice di parità H *di un codice lineare è una matrice* $n \times k$ *tale per cui* $G \cdot H = 0$.

Definizione 17 *Sia* H *la matrice di parità di un codice* C. $\underline{w} \in C$ *se e solo se* $\underline{w}H^T = 0$.

Definizione 18 G *è detta in* forma standard *se* $G = (I_k P)$ *dove* I_k *è la matrice identità* $k \times k$ *e* P *è una matrice* $k \times (n - k)$. *Se* G *è nella forma sistematica o standard allora i primi* k *simboli di una parola sono chiamati simboli di informazione.*

Teorema 19 *Se un codice C $[n,k]$ ha una matrice $G = (I_k P)$ nella forma standard, allora una matrice di parità di C è $H = (-P^T I_{n-k})$ dove P^T è la trasposta di P ed è una matrice $(n-k) \times k$ e I_{n-k} è la matrice identità $(n-k) \times (n-k)$.*

I codici sistematici hanno il vantaggio che il messaggio di dati è presente nella parola codice e può essere letto prima della decodifica. Per codici in forma non sistematica il messaggio non è più riconoscibile nella sequenza codificata ed è necessario avere un invertitore per riconoscere la sequenza di dati.

Definizione 20 *Sia C un codice lineare con matrice di parità H, allora, detta $\underline{x}$ una n-pla binaria $\underline{x}H^T$ si dice* sindrome *di $\underline{x}$.*

Definizione 21 *Il* peso *di un vettore $\underline{u}$ è il numero di componenti diverse da 0.*

Definizione 22 *Il* minimo peso *d di un codice è il peso del vettore diverso da $\underline{0}$ di più piccolo peso nel codice.*

d è dunque una misura della "bontà" di un codice.
Sia definita una sfera $S_r(\underline{u})$ di raggio r intorno ad un vettore $\underline{u}$ come

$$S_r(\underline{u}) = \{\underline{v} \in \mathbf{V} \mid d(\underline{u}, \underline{v}) \leq r\}$$

Teorema 23 *Se d è il peso minimo di un codice C, allora C può correggere al massimo $t = [\frac{d-1}{2}]$ errori e viceversa.*

Corollario 24 *C ha peso minimo d se d è il più grande numero tale che ogni d-1 colonne della matrice di parità H sono indipendenti.*

Si supponga per esempio di voler costruire un codice in forma sistematica che corregga 2 errori. La matrice H sarà costituita dalla matrice identità e da una matrice P^T tale che abbia 4 colonne linearmente indipendenti, cioè il determinante della sottomatrice costituita da queste 4 colonne sia $\neq 0$. Quindi a seconda del numero di errori che si vuole correggere si cerca una

matrice H con $d-1$ colonne linearmente indipendenti. Dunque, dato n e k, si cerca un codice con d il più largo possibile in modo da correggere più errori.
È però possibile che ci siano vettori in $\mathbf{V}$ che non sono contenuti in nessuna di queste sfere.

Definizione 25 *Un codice C di minimo peso d è chiamato* perfetto *se tutti i vettori in $\mathbf{V}$ sono contenuti in sfere di raggio $t = [\frac{d-1}{2}]$ intorno alle parole del codice. In questo caso si dice che le sfere coprono lo spazio.*

Per n e k dati sono i codici migliori.

Teorema 26 *Affinchè un codice binario pefetto $[n,k]$ esista, n,k e t devono soddisfare la seguente equazione*

$$\left(\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{t}\right)2^k = 2^n$$

In generale:

Teorema 27 *Affinchè un codice $[n,k]$ esista, n,k e t devono soddisfare la seguente disuguaglianza nota come disuguaglianza di Hamming:*

$$\left(\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{t}\right)2^k \geq 2^n$$

Quando si riceve la parola y si vuole cercare la parola x che era stata spedita ed in seguito il messaggio di dati c. Si procede nel seguente modo: $y = x + \xi_t \Longrightarrow H(m+\xi_t) = H\xi_t$
dove ξ_t è una particolare classe di errori. Se $H\xi_t \in H$ allora si può dire quale è la posizione errata.
Si supponga che avvenga un errore:
$m + \xi_i \Longrightarrow H(m+\xi_i) = H\xi_i$
$H\xi_i \in H? \longrightarrow$ posizione errata: i
Si supponga ora che avvengano 2 errori:
$m + \xi_i + \xi_j \Longrightarrow H(m+\xi_i+\xi_j) = H\xi_i + H\xi_j = s$
$\forall \xi_i \longrightarrow H\xi_i + H\xi_j \in H? \longrightarrow$ posizioni errate: i e j

Si veda il seguente esempio pratico per codici correttori di un errore (codici di Hamming): si consideri il codice di Hamming $[7, 4]$ descritto dalla seguente matrice generatrice:

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Si considerino le prime 4 posizioni come le posizioni di informazione e le ultime 3 come quelle di ridondanza. Dunque la prima riga rappresenta il messaggio 1 0 0 0 e così via. Tutte le parole si ottengono sommando (mod 2) quelle righe. Per esempio si codifica il messaggio $\underline{u} = (1011)$ come $\underline{x} = (1011010)$.
Si consideri la matrice di parità H:

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Si noti che le colonne della matrice sono state scritte in modo che la i - esima colonna è costituita dai coefficienti di sviluppo di i in base 2, eventualmente completata di 0.
Si supponga di inviare il messaggio $\underline{x}$ di sopra e che ci sia un errore. Si riceva quindi il messaggio $\underline{y} = (1010010)$. Si calcoli la sindrome

$$H \cdot \underline{y}^T = (100)$$

(1 0 0) è la rappresentazione binaria di 4; dunque il bit errato è il quarto.
L'ideale è dunque ricercare dei codici perfetti, ma non sempre si trovano, inoltre si vorrebbero avere dei codici che riconoscano un errore del tipo $0 \longrightarrow 1$ da $1 \longrightarrow 0$.

Pur vantaggiose sotto vari aspetti, le metodologie attualmente in uso richiedono l'aggiunta di una porzione di informazione di ridondanza che fissata la dimensione del singolo messaggio *da codificare* non puo' essere inferiore ad un minimo indicato. Il problema tecnico che sta alla base della presente invenzione è quello di escogitare un codice lineare che protegga un'informazione digitale, codificate come sequenze di simboli binari, superando i limiti delle soluzioni attualmente messe a disposizione dalla tecnica nota.

Sommario dell'Invenzione

L'idea di soluzione che sta alla base dell'invenzione è quella di individuare una codifica per un alfabeto binario in gruppi non booleani, vale a dire in gruppi non binari.

Sulla base di tale idea di soluzione il problema tecnico è risolto da un metodo del tipo precedentemente indicato e definito dalla rivendicazione 1 e seguenti.

Le caratteristiche ed i vantaggi del metodo secondo l'invenzione risulteranno dalla descrizione, fatta qui di seguito, di un esempio di attuazione dato a titolo indicativo e non limitativo.

Descrizione dettagliata

Viene ora descritto nel dettaglio il metodo secondo l'invenzione che applica la teoria dei codici autocorrettori ad informazioni digitali codificate come sequenze di simboli.

Più in particolare, il metodo secondo l'invenzione consente di effettuare correzioni d'errore su informazioni digitali codificate come sequenze $\underline{x}$ di simboli, ad esempio informazioni digitali memorizzate in sistemi di memoria elettronici o trasmesse da e verso tali sistemi e in cui è prevista la trasmissione di sequenze $\underline{x}$ incorporanti una porzione di codice correttore d'errore che consenta di ricostruire in ricezione la sequenza $\underline{x}$ che più probabilmente è l'originale trasmessa mediante il calcolo di una sindrome d'errore utilizzando una matrice di parità.

Vantaggiosamente, il metodo prevede che il codice d'errore incorporato nella sequenza $\underline{x}$ originaria appartenga ad un gruppo non booleano.

Il codice d'errore utilizzato è un codice lineare, come risulterà dalla seguente dettagliata descrizione delle modalità di attuazione del metodo.

0.2 Codici su gruppi diversi

Si considerino gruppi additivi. Il gruppo dove si è lavorato con i codici precedenti è booleano, cioè detto x un elemento del campo si ha che $x + x =$ identità rispetto alla somma. Ora si considerino gruppi additivi $\pmod p$ con $p \in \mathbb{N}$.
Si cercano dei codici analoghi a quelli descritti sopra, cioè codici per i quali detta H la matrice di parità del codice e y la parola ricevuta si abbia:

$$y \cdot H^T = 0$$

se y è una parola del codice. Si cercano dunque codici lineari. Inoltre se y è affetta da uno o più errori si vuole che:

$$(y + \xi_i + \xi_j) \cdot H^T = \xi_i \cdot H^T + \xi_j \cdot H^T = s_i + s_j$$

dove s_i ed s_j sono le colonna i-esima e j-esima della matrice H^T. Il codice cercato deve dunque appartenere ad un gruppo abeliano per avere questa proprietà.
Si cercano codici in forma sistematica e si vede come costruire la matrice identità. Si considerano le colonne come numeri scritti in base 10. La matrice diverrà dunque un vettore di numeri ed il prodotto matrice per messaggio ricevuto diverrà un prodotto scalare. Operando in un gruppo $\pmod p$ i numeri costituenti la matrice identità devono essere tali che la matrice costituita dalla loro rappresentazione binaria abbia determinante $\neq 0$. Fissato $n - k$ il numero di bit di parità si sceglie p tale che:

$$2^{n-k} + 1 \leq p \leq 2^{n-k+1} - 1$$

La matrice identità è costituita dai numeri $p - 1, p - 2, \cdots, p - 2^{n-k}$. Si consideri un codice C $[7, 4]$ con $p = 8$, la matrice idenità sarà costituita dai numeri 7,6 e 4. La matrice scritta in binario sarà dunque della forma:

$$I_2 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

contro la solita matrice identità:

$$I_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

rappresentata dai numeri in base 10: 1, 2 e 4.
Si noti che si potrebbe scegliere una qualsiasi matrice tale che abbia "determinante" $\neq 0$ cioè un numero appartenente a quella matrice non sia combinazione lineare di altri numeri appartenenti a quella matrice. Questa scelta risulta particolarmente efficiente. Si può vedere con un esempio.
Si supponga che il prodotto di un vettore di dati per una certa matrice P ($H = (P, I)$) abbia dato come risultato 1 , che scritto in binario come 100 costituerà la parte di codice da aggiungere alla parola. m è visto come un vettore di pesi c_i; dunque, detti x_i i numeri costituenti la matrice H (vista come un vettore):

$$m \cdot H = \sum_{i=1}^{n} c_i x_i \qquad c_i = 0, 1$$

dove la somma è fatta $\pmod p$. Quando si riceve il messaggio si deve moltiplicare $m \cdot H^T$ cioè $(m_k, m_{n-k}) \cdot (P, I) = m_k \cdot P + m_{n-k} \cdot I$. In questo caso il primo valore è 1 ed affinchè il messaggio sia corretto deve essere:

$$1 + m_{n-k} \cdot I = 0 \pmod p$$

Si scelga come matrice identità quella usuale cioè $[1, 2, 4]$. Si ha:

$$[1, 2, 4] \cdot (c_1, c_2, c_3) + 1 = 0$$

Lavorando in un campo $\mathbb{Z}_8$ invece di avere 0 a secondo membro si può avere $8k$ con $k \in \mathbb{N}$. La soluzione è $(c_1, c_2, c_3) = (111)$.
Si scelga ora come matrice quella proposta, cioè $[7, 6, 4]$. Si ha:

$$[7, 6, 4] \cdot (c_1, c_2, c_3) + 1 = 0$$

La soluzione è $(c_1, c_2, c_3) = (100)$, cioè lo stesso valore del codice calcolato. Questo fatto non è casuale, con la matrice identità proposta il codice calcolato

è sempre uguale al codice ricevuto se non sono avvenuti errori.
I numeri costituenti le colonne della matrice di parità P dovranno essere scelti secondo i criteri analoghi a quelli del gruppo booleano.
Con codici in questi gruppi viene distinto l'errore $1 \rightarrow 0$ da $0 \rightarrow 1$, quindi il canale non è più simmetrico. Difatti:

- se la sindrome restituisce un valore x con $x \in H$ l'errore avvenuto è $0 \rightarrow 1$;
- se la sindrome restituisce un valore x con $x \notin H$, ma $p - x \in H$ allora l'errore avvenuto è $1 \rightarrow 0$;

Si assegni un errore +1 al primo caso ed un errore -1 al secondo caso.
Si consideri un codice $[6, 1]$ con $p = 22$.

$$H = (11 \mid 21\,20\,18\,14\,6)$$

In binario questa matrice sarà:

$$H = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}$$

le parole codice saranno dunque:

$$0 \mid 00000$$

$$1 \mid 11010$$

Si invii la seconda parola del codice, ma si riceva 111110 cioè è avvenuto un errore +1 nella quarta posizione. Si calcoli: $(111110) \cdot H = 1 \cdot 11 + 1 \cdot 21 + 1 \cdot 20 + 1 \cdot 18 + 1 \cdot 14 = 84$ che nel gruppo che si sta considerando è 18. 18 c'è nella matrice H e dunque l'errore avvenuto è $0 \rightarrow 1$, inoltre 18 si trova nella quarta posizione della matrice che è la posizione errata nel messaggio.

Si supponga ora di avere ricevuto 101010 cioè è avvenuto un errore -1 nella seconda posizione. Si calcoli: $(101010) \cdot H = 1 \cdot 11 + 1 \cdot 20 + 1 \cdot 14 = 45$ che nel gruppo considerato è 1. 1 non c'è nella matrice H, ma c'è $22 - 1 = 21$ e dunque l'errore avvenuto è $1 \rightarrow 0$, inoltre 21 si trova nella seconda posizione della matrice che è la posizione errata nel messaggio.
Si osservi che gli errori nel messaggio ricevuto possono essere solo di un tipo, o +1 o -1 in ogni posizione, a seconda che il bit corrispondente sia 0 o 1 nel messaggio ricevuto. Se si rileva un errore impossibile significa che il codice è stato in grado di diagnosticare ma non di correggere gli errori.
Si veda un esempio contraddittorio.
Si consideri un codice [3, 1] in un gruppo (mod 4) dove la matrice $H = (1 \mid 3\,2)$. Le parole del codice saranno:

$$0 \mid 00 \quad 1 \mid 10$$

Si spedisca il messaggio 000 e si riceva 010.

$$(010) \cdot H = 3$$

3 è presente nella matrice e ciò indicherebbe un errore +1 nella seconda posizione. $4 - 3 = 1$ che è anch'esso nella matrice e ciò indica un errore -1 nella prima posizione. Difatti 010 può essere ottenuto anche da 110 con un errore nella prima posizione. Quindi non si riesce a trovare un codice su $\mathbb{Z}_4$
Talvolta per poter correggere gli errori è necessario non solo calcolare la sindrome ma anche confrontare i bit ricevuti. Si consideri un codice [3, 1] su $\mathbb{Z}_5$ con matrice $H = (3 \mid 4\,3)$. Le parole codice saranno:

$$0 \mid 00 \quad 1 \mid 11$$

Si spedisca la parola 000, si considerino tutti gli errori che possono accadere e la decodifica.

- 001 $\Longrightarrow$ sindrome = 3. Errori possibili:

  1) +1 nella prima posizione;

2) +1 nella terza posizione;

Dato che si è ricevuto uno 0 nella prima posizione, il caso 1 non è possibile.

- 010 $\Longrightarrow$ sindrome = 4. Errore possibile: +1 nella seconda posizione.
- 100 $\Longrightarrow$ sindrome = 3. Errori possibili:

  1) +1 nella prima posizione;

  2) +1 nella terza posizione;

  Dato che si è ricevuto uno 0 nella terza posizione, il caso 2 non è possibile.

Si spedisca ora la parola 111, si considerino tutti gli errori che possono accadere e la decodifica.

- 011 $\Longrightarrow$ sindrome = 2. Errori possibili:

  1) -1 nella prima posizione;

  2) -1 nella terza posizione;

  Dato che si è ricevuto un 1 nella terza posizione, il caso 2 non è possibile.

- 101 $\Longrightarrow$ sindrome = 1. Errore possibile: -1 nella seconda posizione.
- 110 $\Longrightarrow$ sindrome = 2. Errori possibili:

  1) -1 nella prima posizione;

  2) -1 nella terza posizione;

  Dato che si è ricevuto un 1 nella prima posizione, il caso 1 non è possibile.

In queso modo si distingue il tipo di errore avvenuto, confrontando la sindrome con i valori effettivamente ricevuti. La realizzazione di un circuito che

descriva questo metodo comporta la creazione di addizionatori non binari, anche se lavorano con sequenza di 0 e 1 (scrivendo ogni numero con la rappresentazione binaria). Se per esempio lavoriamo su $\mathbb{Z}_5$ l'addizionatore deve saper dire che $(100)+(100) = (010)$ cioè $1+1 = 2$, ma $(110)+(010) = (000)$, cioè $3 + 2 = 5$. Inoltre si deve essere in grado di fare il complemento di un numero che andrà ricercato nella matrice.

RIVENDICAZIONI

1. Metodo per effettuare correzioni d'errore su informazioni digitali codificate come sequenze (x) di simboli, ad esempio informazioni digitali memorizzate in sistemi di memoria elettronici o trasmesse da e verso tali sistemi e in cui è prevista la trasmissione di sequenze (x) incorporanti una porzione di codice correttore d'errore che consenta di ricostruire in ricezione la sequenza (x) che più probabilmente è l'originale trasmessa mediante il calcolo di una sindrome d'errore utilizzando una matrice di parità, caratterizzato dal fatto che il codice d'errore incorporato nella sequenza (x) originaria appartiene ad un gruppo non booleano.

2. Metodo secondo la rivendicazione 1, caratterizzato dal fatto che detto codice d'errore è un codice lineare.

3. Metodo secondo la rivendicazione 1, caratterizzato dal fatto che detto codice d'errore riconosce un errore del tipo $0 \rightarrow 1$ da un errore del tipo $1 \rightarrow 0$.

4. Metodo secondo la rivendicazione 1, caratterizzato dal fatto che detta matrice di parità contiene una matrice d'identità avente un determinante diverso da 0, vale a dire che un numero appartenente alla matrice non è combinazione lineare di altri numeri appartenenti alla stessa matrice e se in un gruppo additivo mod p con p diverso da 2 è costituita dai numeri p-1, p-2,.., $p-2^{n-k}$.

5. Metodo secondo la rivendicazione 1, caratterizzato dal fatto che detto codice d'errore appartiene ad un gruppo abeliano.

6. Metodo secondo la rivendicazione 1, caratterizzato dal fatto che detto codice d'errore è un codice in forma sistematica.

RIASSUNTO

Si descrive un metodo per effettuare correzioni d'errore su informazioni digitali codificate come sequenze (x) di simboli, ad esempio informazioni digitali memorizzate in sistemi di memoria elettronici o trasmesse da e verso tali sistemi e in cui è prevista la trasmissione di sequenze (x) incorporanti una porzione di codice correttore d'errore che consenta di ricostruire in ricezione la sequenza (x) che più probabilmente è l'originale trasmessa mediante il calcolo di una sindrome d'errore utilizzando una matrice di parità.

Vantaggiosamente secondo l'invenzione, il codice d'errore incorporato nella sequenza (x) originaria appartiene ad un gruppo non booleano.